

Substitute for form 1449/PTO

# INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known

Application Number	09/540611
Filing Date	March 31, 2000
First Named Inventor	Ellison, Carl
Group Art Unit	Unknown
Examiner Name	Unknown

Sheet 1 of 1

Attorney Docket No: 42P08112

## FOREIGN PATENT DOCUMENTS

Examiner Initials*	Foreign Document No	Publication Date	Name of Patentee or Applicant of cited Document	Class	Subclass	T <sup>2</sup>
	JP-JP2000076139	03/14/2000	Tanno, Masaaki, et al.			
ECT	WO-WO0175564	10/11/2002	Herbert, Howard C., et al.			
↓	WO-WO02086684	10/31/2002	Proudlar, Graeme J.			
	WO-WO0217555	02/28/2002	Ford, Warwick			

## OTHER DOCUMENTS -- NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No <sup>1</sup>	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T <sup>2</sup>
ECT		CHIEN, ANDREW A., et al., "Safe and Protected Execution for the Morph/AMRM Reconfigurable Processor", 7th Annual IEEE Symposium, FCCM '99 Proceedings, XP010359180, ISBN 0-7695-0375-6, Los Alamitos, CA, (4/21/1999), 209-221	
↓		COMPAQ COMPUTER CORPORATION, et al., "Trusted Computing Platform Alliance (TCPA) Main Specification Version 1.1a", (12/2001), 1-321	
		IBM, "Information Display Technique for a Terminate Stay Resident Program IBM Technical Disclosure Bulletin", TDB-ACC-No. NA9112156, Vol. 34, Issue 7A, (12/1/1991), 156-158	
		KARGER, PAUL A., et al., "A VMM Security Kernel for the VAX Architecture", Proceedings of the Symposium on Research in Security and Privacy, XP010020182, ISBN 0-8186-2060-9, Boxborough, MA, (5/7/1990), 2-19	
↓		ROBIN, JOHN S., et al., "Analysis of the Pentium's Ability to Support a Secure Virtual Machine Monitor", Proceedings of the 9th USENIX Security Symposium, XP002247347, Denver, Colorado, (8/14/00), 1-17	

EXAMINER

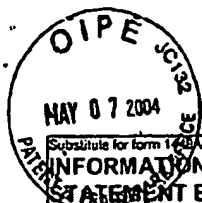
EE Jim

DATE CONSIDERED

2 MAR '06

Substitute Disclosure Statement Form (PTO-1449)

\* EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). Applicant is to place a check mark here if English language Translation is attached



Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it carries a valid OMB control number.

Substitute for form 1-618 APTO  
**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**  
(Use as many sheets as necessary)

Complete if Known	
Application Number	09/540611
Filing Date	March 31, 2000
First Named Inventor	Ellison, Carl
Group Art Unit	Unknown
Examiner Name	Unknown

**RECEIVED**

MAY 11 2004

Sheet 1 of 1

Attorney Docket No: 42P08112

Technology Center 2100

**FOREIGN PATENT DOCUMENTS**

Examiner Initials*	Foreign Document No	Publication Date	Name of Patentee or Applicant of cited Document	Class	Subclass	T*
ECR	JP-JP2000076139	03/14/2000	Tanno, Masaaki, et al.			
	WO-WO0175564	10/11/2002	Herbert, Howard C., et al.			
	WO-WO02086684	10/31/2002	Proudlar, Graeme J.			
	WO-WO0217555	02/28/2002	Ford, Warwick			

**OTHER DOCUMENTS -- NON PATENT LITERATURE DOCUMENTS**

Examiner Initials*	Cite No*	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T*
ECT		CHIEN, ANDREW A., et al., "Safe and Protected Execution for the Morph/AMRM Reconfigurable Processor", 7th Annual IEEE Symposium, FCCM '99 Proceedings, XP010359180, ISBN 0-7695-0375-6, Los Alamitos, CA, (4/21/1999), 209-221	
		COMPAQ COMPUTER CORPORATION, et al., "Trusted Computing Platform Alliance (TCPA) Main Specification Version 1.1a", (12/2001), 1-321	
		IBM, "Information Display Technique for a Terminate Stay Resident Program IBM Technical Disclosure Bulletin", TDB-ACC-No. NA9112156, Vol. 34, Issue 7A, (12/1/1991), 156-158	
		KARGER, PAUL A., et al., "A VMM Security Kernel for the VAX Architecture", Proceedings of the Symposium on Research in Security and Privacy, XP010020182, ISBN 0-8186-2060-9, Boxborough, MA, (5/7/1990), 2-19	
		ROBIN, JOHN S., et al., "Analysis of the Pentium's Ability to Support a Secure Virtual Machine Monitor", Proceedings of the 9th USENIX Security Symposium, XP002247347, Denver, Colorado, (8/14/00), 1-17	

EXAMINER

*PT Lu*

DATE CONSIDERED

10 Aug '04

Substitute Disclosure Statement Form (PTO-1449)

\* EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 608. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional) Applicant is to place a check mark here if English language Translation is attached

Substitute for form 1449A/PTO  
**INFORMATION DISCLOSURE  
 STATEMENT BY APPLICANT**  
 (Use as many sheets as necessary)



Sheet 1 of 2

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it carries a valid OMB control number.

PTO/SB/PM (10-01)  
 Approved for use through 10/1/2002, OMB 051-0001  
 US Patent & Trademark Office U.S. DEPARTMENT OF COMMERCE

Complete if Known	
Application Number	09/540,611
Filing Date	March 31, 2000
First Named Inventor	Ellison, Carl
Group Art Unit	2134
Examiner Name	Tran, Ellen
Attorney Docket No: 42P08112	

**FOREIGN PATENT DOCUMENTS**

Examiner Initials*	Foreign Document No	Publication Date	Name of Patentee or Applicant of cited Document	Class	Subclass	T <sup>2</sup>
ELS	EP-EP0892521	01/20/1999	Zamek, Steven			
	EP-EP1055989	11/29/2000	Proudlar, Graeme J., et al.			
	EP-EP1056014	11/29/2000	Proudlar, Graeme J., et al.			
	WO-WO0201794	01/03/2002	Ellison, Carl			
	WO-WO02060121	08/01/2002	Grawrock, David W.			
	WO-WO03058412	07/17/2003	Glew, Andrew, et al.			
	WO-WO9812620	03/26/1998	Nishiuchi, Taiki, et al.			
	WO-WO9918511	04/15/1999	Edrich, David R.			

**OTHER DOCUMENTS – NON PATENT LITERATURE DOCUMENTS**

Examiner Initials*	Cite No <sup>1</sup>	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T <sup>2</sup>
ECT		COULOURIS, GEORGE, et al., "Distributed Systems, Concepts and Designs", 2nd Edition, (1994), 422-424	
		CRAWFORD, JOHN, "Architecture of the Intel 80386", <u>Proceedings of the IEEE International Conference on Computer Design: VLSI in Computers and Processors (ICCD '86)</u> , (October 6, 1986), 155-160	
		FABRY, R.S., "Capability-Based Addressing", Fabry, R.S., "Capability-Based Addressing", <u>Communications of the ACM</u> , Vol. 17, No. 7, (July 1974), 403-412	
		FRIEDER, GIDEON, "The Architecture And Operational Characteristics of the VMX Host Machine", <u>The Architecture And Operational Characteristics of the VMX Host Machine</u> , IEEE, (1982), 9-16	
		INTEL CORPORATION, "IA-64 System Abstraction Layer Specification", <u>Intel Product Specification</u> , Order Number 245359-001, (01/2000), 1-112	
		INTEL CORPORATION, "Intel IA-64 Architecture Software Developer's Manual", <u>Volume 2: IA-64 System Architecture</u> , Order Number 245318-001, (01/2000), i, ii, 5.1-5.3, 11.1-11.8, 11.23-11.26	
		MENEZES, ALFRED J., et al., "Handbook of Applied Cryptography", <u>CRC Press Series on Discrete Mathematics and its Applications</u> , Boca Raton, FL, XP002165287, ISBN 0849385237, (Oct. 1996), 403-405, 506-515, 570	
		NANBA, S., et al., "VM/4: ACOS-4 Virtual Machine Architecture", <u>VM/4: ACOS-4 Virtual Machine Architecture</u> , IEEE, (1985), 171-178	
		RSA SECURITY, "Hardware Authenticators", <u>www.rsasecurity.com/node.asp?id=1158</u> , 1-2	
		RSA SECURITY, "RSA SecurID Authenticators", <u>www.rsasecurity.com/products/securid/datasheets/SID_DS_0103.pdf</u> , 1-2	
		RSA SECURITY, "Software Authenticators", <u>www.rsasecurity.com/node.asp?id=1313</u> , 1-2	

EXAMINER

*C P L* DATE CONSIDERED *0 Apr '04*

Substitute Disclosure Statement Form (PTO-1449)

\* EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 608. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). Applicant to place a check mark here if English language Translation is attached

RECEIVED  
MAR 30 2000  
E

PTO/SB08A(10-01)  
Approved for use through 10/31/2002. OMB 051-0001  
US Patent & Trademark Office, U.S. DEPARTMENT OF COMMERCE

#  
14P

Substitute for form 1449A/PTO  
**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**  
(Use as many sheets as necessary)

RECEIVED  
JAN 30 2004  
E

Complete if Known	
Application Number	09/540611
Filing Date	March 31, 2000
First Named Inventor	Ellison, Carl
Group Art Unit	Unknown
Examiner Name	Unknown
Attorney Docket No: 42P08112	

Sheet 1 of 1

**FOREIGN PATENT DOCUMENTS**

Examiner Initials*	Foreign Document No	Publication Date	Name of Patentee or Applicant of cited Document	Class	Subclass	T <sup>2</sup>
ECR	JP-JP2000076139	03/14/2000	Tanno, Masaaki, et al.			
	WO-WO0175564	10/11/2002	Herbert, Howard C., et al.			
	WO-WO02086684	10/31/2002	Proudlar, Graeme J.			
	WO-WO0217555	02/28/2002	Ford, Warwick			

**OTHER DOCUMENTS -- NON PATENT LITERATURE DOCUMENTS**

Examiner Initials*	Cite No <sup>1</sup>	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T <sup>2</sup>
ECR	/	CHIEN, ANDREW A., et al., "Safe and Protected Execution for the Morph/AMRM Reconfigurable Processor", 7th Annual IEEE Symposium, FCCM '99 Proceedings, XP010359180, ISBN 0-7695-0375-6, Los Alamitos, CA, (4/21/1999), 209-221	
	/	COMPAQ COMPUTER CORPORATION, et al., "Trusted Computing Platform Alliance (TCPA) Main Specification Version 1.1a", (12/2001), 1-321	
	/	IBM, "Information Display Technique for a Terminate Stay Resident Program IBM Technical Disclosure Bulletin", TDB-ACC-No. NA9112156, Vol. 34, Issue 7A, (12/1/1991), 156-158	
	/	KARGER, PAUL A., et al., "A VMM Security Kernel for the VAX Architecture", Proceedings of the Symposium on Research in Security and Privacy, XP010020182, ISBN 0-8186-2060-9, Boxborough, MA, (5/7/1990), 2-19	
	/	ROBIN, JOHN S., et al., "Analysis of the Pentium's Ability to Support a Secure Virtual Machine Monitor", Proceedings of the 9th USENIX Security Symposium, XP002247347, Denver, Colorado, (8/14/00), 1-17	

RECEIVED

FEB 03 2004

Technology Center 2100

EXAMINER

ECR

DATE CONSIDERED

10 Apr '04

Substitute Disclosure Statement Form (PTO-1449)  
\* EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. 1 Applicant's unique citation designation number (optional) 2 Applicant is to place a check mark here if English language Translation is attached

09/540,611

09/540 611

ECT

Reference No.	Application Serial No.	Patent No.	Title
1	09/672,603		Controlling Accesses To Isolated Memory Using A Memory Controller For Isolated Execution
2	09/822,986		Checking File Integrity Using Signature Generated In Isolated Execution
3	09/538,951		Platform And Method For Issuing And Certifying A Hardware-Protected Attestation Key
4	09/539,344		Managing A Secure Platform Using A Hierarchical Executive Architecture In Isolated Execution Mode
5	09/668,585		Managing A Secure Platform Using A Hierarchical Executive Architecture In Isolated Execution Mode
6	09/541,108		Platform And Method For Remote Attestation Of A Platform
7	09/540,612		Platform And Method For Generating And Utilizing A Protected Audit Log
8	09/540,946		Protecting Software Environment In Isolated Execution
9	09/668,610		Protecting Software Environment In Isolated Execution
10	09/538,954		Generating Isolated Bus Cycles For Isolated Execution
11	09/539,348	6,760,441	Generating A Key Hierarchy For Use In An Isolated Execution Environment
12	09/541,477	6,507,904	Isolated Instructions For Isolated Execution
13	09/540,611		Managing Accesses In A Processor For Isolated Execution
14	09/540,613		Managing A Secure Environment Using A Chipset In Isolated Execution Mode
15	09/668,408		Managing A Secure Environment Using A Chipset In Isolated Execution Mode
16	09/541,667		Attestation Key Memory Device And Bus
17	09/672,602		Attestation Key Memory Device And Bus
18	09/618,738	6,678,825	Controlling Access To Multiple Isolated Memories In An Isolated Execution Environment
19	09/618,489	6,633,963	Controlling Access To Multiple Memory Zones In An Isolated Execution Environment
20	10/683,542		Controlling Access To Multiple Memory Zones In An Isolated Execution Environment
21	09/618,659		Resetting A Processor In An Isolated Execution Environment
22	09/751,586		Resetting A Processor In An Isolated Execution Environment

26 FEB '05

EL Tran